Group Centric Networking: Addressing Information Sharing Requirements at the Tactical Edge

Bow-Nan Cheng, Greg Kuperman, Patricia Deutsch, Logan Mercer, Aradhana Narula-Tam
MIT Lincoln Laboratory
{bcheng, gkuperman, patricia.deutsch, logan.mercer, arad}@ll.mit.edu

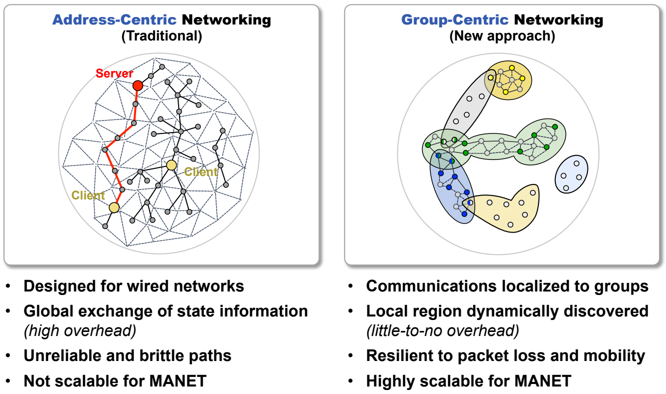
***Abstract*—In recent years, there's been a large push in the U.S. Department of Defense to move to an all Internet Protocol (IP) infrastructure, particularly on the tactical edge. IP and associated protocols were designed primarily for wired networks tied to fixed infrastructure. Although extensions to support mobile ad hoc networking (MANET) have received decades of research, in practice, there are few successful implementations. Challenges include handling mobility, managing lossy links, and scaling to large numbers of users. Unfortunately, these are the exact conditions military tactical edge networks must operate within: high mobility, high loss, and large numbers of users.**

To address the needs and particular challenges of military tactical edge information sharing requirements, we consider a new class of networking approaches called group-centric networks that focuses on dynamic and resilient formation of interest groups. The structure of tactical networks limits the majority of collaboration and network traffic to within a group of users that share a set of common interests (i.e. platoons, 4-ships, etc.). These groups are formed either prior to the mission or on-the-fly with only a minor amount of traffic flowing outside of these groups. Group centric networking approaches can help connect users in military tactical edge networks. In addition, we also discuss an instantiation of a group-centric network protocol called Group Centric Networking (GCN), compare GCN against a traditional MANET routing approaches on a 90 node Android mobile phone testbed, and discuss implications for tactical edge users.

I. Introduction

In recent years, there's been a large push in the U.S. Department of Defense to move to an all Internet Protocol (IP) infrastructure, particularly on the tactical edge [1]. Tactical edge networks [2] like Link 16 [3] and others have traditionally been vertically integrated and rely on tight coupling between host computer and radio in terms of time slot assignments, message sizes, etc. Specific message sets that are defined per system and the host computer send these messages at the exact time the radio expects the message. In contrast, IP networks converge at the network layer, enabling multiple applications to ride over the network without knowing details of the underlying network and physical medium. This effectively decouples applications from radios and enables greater interoperability and allows for radio and application technologies to evolve at different rates.

While IP technologies dominate the commercial sector, its success at the tactical edge has been limited. IP networks function well with fixed infrastructure and stable links where routes are maintained to enable all-to-all unicast connections. While cellular networks and sensor networks have seen success in moving to IP, almost all wireless links are direct connections to fixed infrastructure and have little to no mobility. In contrast, military tactical edge networks are mobile and must operate without infrastructure and in disruption, interference, and lossy environments. Additionally, military force structure limits the majority of collaboration and network traffic within groups (i.e. platoons, 4-ships, etc.) that are formed either prior to the mission or on-the-fly. These groups are typically geographically localized to three or fewer radio frequency (RF) hops [4].



- Designed for wired networks
- Global exchange of state information *(high overhead)*
- Unreliable and brittle paths
- Not scalable for MANET

- Communications localized to groups
- Local region dynamically discovered *(little-to-no overhead)*
- Resilient to packet loss and mobility
- Highly scalable for MANET

Fig. 1: Address-centric networking technologies do not fulfill requirements of group-centric military networks

To address the needs of military tactical edge information sharing requirements, we consider a new class of networking approaches called group-centric networks that was first proposed in [5]. These group-centric networks focuses on dynamic formation of interest groups to support one-to-many (traditional multicast), many-to-many (shared view), one-to-one (traditional unicast), and many-to-one (exfiltration) types of traffic. This is the exact type of traffic that is existent in military networks. In particular, a group-centric network has the following characteristics:

1) Users/Applications are grouped by an inherent set of "interests" that are dependent on the tasks they are performing, and these group members will wish to communicate reliably between one another. Devices are

Distribution A: Public Release; unlimited distribution. This work is sponsored by the Defense Advanced Research Projects Agency under Air Force Contract #FA8721-05-C-0002. The views, opinions, and/or findings expressed are those of the author(s) and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

not limited to a single group, and can belong to multiple groups.

2) The majority of message exchanges are be within some local area with limited long-distance traffic.
3) Any device can be a source or a sink, and traffic patterns between them may be one-to-one, one-to-many, many-to-one, or many-to-many.
4) Future wireless environments will have a mix of mobile and stationary devices, where mobility will be typically be limited to some local area.

Figure 1 illustrates the high level difference between IP networks which are address-centric to group-centric networks. In traditional address-centric networks, multiple clients connect to a server to pull or exchange data. As an example, multiple web browsers (clients) connect to a web server to view content. Address-centric networks were designed for wired networks where the links are both stable and have high-capacity. Routing protocols for these networks work by constantly maintaining all-to-all routes from every potential client to every potential server. While this approach has been effective in wired networks, in multi-hop, mobile wireless networks, the exchange of state information required to maintain all-to-all unicast paths results in high overhead, which ultimately limits network scalability. Additionally, due to packet loss and mobility, these routing protocols in a multi-hop wireless network result in brittle and unreliable paths.

In group-centric networks, however, interest groups are dynamically discovered and formed based on information sharing needs with little to no overhead. When these groups are formed, communications is localized to the groups which, in turn, are often geographically localized. Instead of building paths to share information which need to be maintained regularly, group-centric networks leverage the broadcast nature of radio systems and dynamically elects relays to "cover" an area with transmissions. As long as nodes move within the coverage area, they will be able to continue receiving transmissions. This results in group-centric networks providing high resiliency to packet loss and mobility in a highly scalable manner. In [5], the authors present Group Centric Networking (GCN), which is a protocol designed specifically for group-centric networks.

In this paper, we examine Group Centric Networking (GCN) and consider its ability to enable military tactical edge networks to collaborate and share information in a group-centric, resilient, and scalable manner. To further understand its practical usability, we instantiate and demonstrate the core GCN technology on a 90 node Android mobile phone network and compare it against several IP unicast and multicast mobile adhoc networking (MANET) technologies. We then assess the applicability of GCN on military tactical edge networks and discuss some limitations and additional considerations. The paper is organized in the following manner: Section II overviews the major mechanisms that enable GCN. Section III presents a summary result of GCN performance compared to other MANET protocols in a 90 node Android mobile phone network. Section IV discusses the implications and limitations of GCN as it applies to tactical edge networks, and finally, Section V concludes the paper with future work.

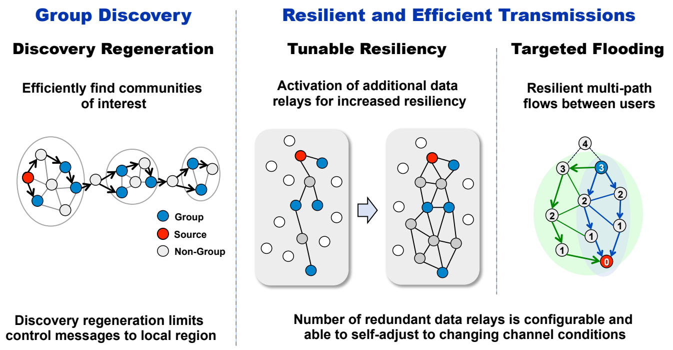

Group Discovery
Resilient and Efficient Transmissions
Discovery Regeneration
Tunable Resiliency
Targeted Flooding
Efficiently find communities of interest
Activation of additional data relays for increased resiliency
Resilient multi-path flows between users
Group
Source
Non-Group
4
3
3
2
2
2
1
1
1
0
Discovery regeneration limits control messages to local region
Number of redundant data relays is configurable and able to self-adjust to changing channel conditions

Fig. 2: GCN is made up of three major mechanisms: 1) group discovery, 2) tunable resiliency, and 3) targeted flooding

II. Group Centric Networking

Group Centric Networking (GCN) [5] is an instantiation of a group-centric network that enables scalable, efficient, and resilient group communications and was designed to enable a group of devices or users to communicate in a local region. In this section, we briefly overview the protocol presented in [5].

The primary design goals of GCN is to be able to (1) efficiently and dynamically discover nodes that have interest in the data (i.e. group nodes) and (2) disseminate information between group nodes in a resilient (against packet errors, interference, and mobility) and bandwidth efficient manner. GCN achieves this through three major high level mechanisms as shown in Figure 2:

1) *Group discovery*: Enables efficient discovery and connection of the local region where group members reside without the use of global control information. This is achieved with a novel *discovery regeneration* algorithm described in Section II-A.
2) *Tunable resiliency*: Provides application-adjusted resiliency towards both packet loss and mobility without the need for constant exchange of control information. This is achieved by activating relay nodes to self-adjust to real-time channel conditions such that the local region is sufficiently "covered". Details of the mechanism is highlighted in Section II-B.
3) *Targeted flooding*: Adds additional resiliency between sets of group members. This is achieved through a gradient-based mechanism that builds a corridor of flooding and is described in Section II-C.

In the following subsections, we provide details on the core mechanisms that form Group Centric Networking (GCN).

A. Group Discovery

The first step to enable GCN is to identify nodes interested in participating in the group (i.e. group nodes). The purpose of the group discovery mechanism is to find and connect group members in a local region without prior knowledge of where those group members reside, and to do so efficiently without globally flooding control messages. In traditional networks, discovery is typically performed by flooding a control message across the network and awaiting replies of interest. The network reach of these discovery messages are typically limited by setting a time-to-live (TTL) field which is decremented at every hop. While the mechanism is straightforward, it is difficult to know the network diameter to cover all group nodes, resulting in the need to set a large TTL. In a large network with limited bandwidth, this can be a significant waste of network resources as the message travels to areas where groups do not exist.

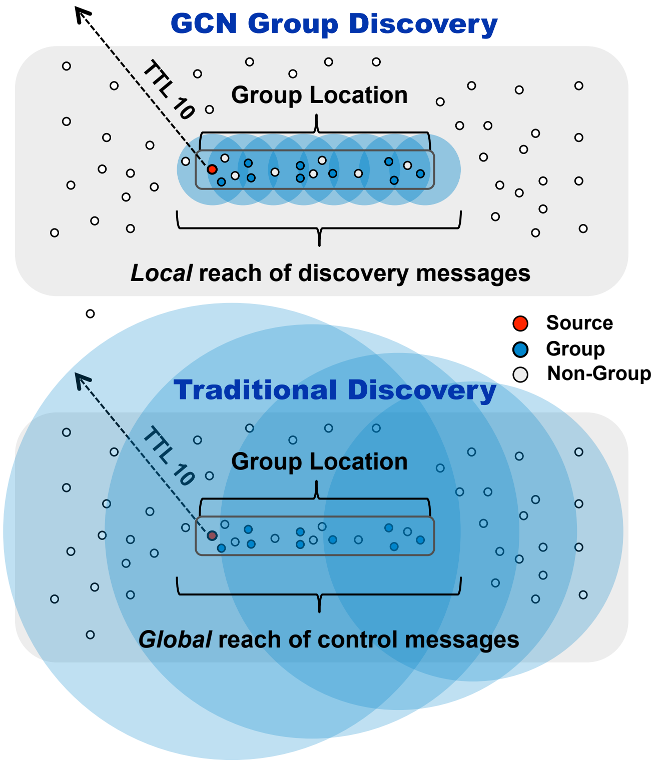


Fig. 3: GCN group discovery limits discovery messages to local corridor of group nodes compared to traditional approaches

For group discovery, GCN introduces a novel approach called *discovery regeneration*, where a group discovery message is regenerated with some small “source” TTL by each group member. Each group node that receives this discovery message resets the TTL to the “source” TTL, retransmits the message, and sends an acknowledgement (ACK) back to the *previous* group node that relayed the discovery message. Non-group nodes retransmit the discovery messages if the TTL is greater than zero. This approach is different from traditional multicast whereby *join* messages are sent to the root of the tree. Duplicate detection is applied by all users in the network to ensure discovery messages are relayed only once. After the group discovery process completes, no link-state or neighbor information is maintained by any user in GCN.

As an example, a source node may set the “source” TTL of a group discovery message to two. If non-group nodes receive the discovery message, it decrements the TTL and relays the message if the TTL is not zero. If a group node receives the message, it resets the TTL to the “source” TTL value and retransmits the message while concurrently sending an ACK message back to the previous group node. The result is that the reach of the discovery message is limited to a fixed distance around the group nodes. Figure 3 highlights the difference between the traditional TTL-based approach and the GCN discovery approach. GCN discovery only floods in the corridor where group nodes reside compared to traditional TTL-based flooding to achieve the percentage of discovery. In theoretical and simulation evaluations, depending on density of group nodes to network nodes, setting a source TTL to three sufficiently discovers all group nodes even for a 5% density of group nodes. Detailed theoretical and simulation evaluation can be found in [5].

B. Tunable Resiliency

While group discovery activates an efficient set of relays such that all group members are connected, this minimal set of relays is not particularly robust for group-wide dissemination as a single packet failure can cause all downstream group members to not receive the data. The issue is exacerbated by varying wireless channel conditions and mobility. To make GCN more robust, group discovery is extended by adding a mechanism called *tunable resiliency*, which enables targeted activation of additional relays to provide additional coverage.

In the group discovery process, an ACK is addressed to a next-hop node to activate as a relay. This node is labeled the *obligate* relay and will always relay messages for the group. Tunable resiliency enables other nodes to self-select based on a desired density of relays. This is achieved by adding a short delay to the discovery acknowledgement (ACK) messages and keeping count of the number of discovery messages overheard from neighbors. Adding a short delay to the ACK responses to group discovery messages enables discovery messages to propagate through the immediate vicinity of a particular user. Having an estimate of the number of nodes in a neighborhood enables nodes to self-select as data relays in a probabilistic manner to achieve a desired density of relays to enable robust data coverage. The details of selection algorithm can be found in [5].

Probabilistically selecting data relays based on number of overheard discovery messages allows the network to self-adjust to real-time error conditions as the number of discovery messages heard by each node reflects the current error rate being experienced in the network. For example, assuming a 50% packet error rate due to interference or some other loss, if ten neighbors of user transmit a discovery message, then on average five of those messages should be expected to be overheard. Users and applications can specify a desired resiliency which would cause a certain number of relays to be self-selected based on the overheard discovery messages.

Figure 4 shows an example of tunable resiliency. Increasing the desired resiliency value activates more relays between group nodes and thickens the network to allow data to cover more of the group area. The result is increased resiliency of the

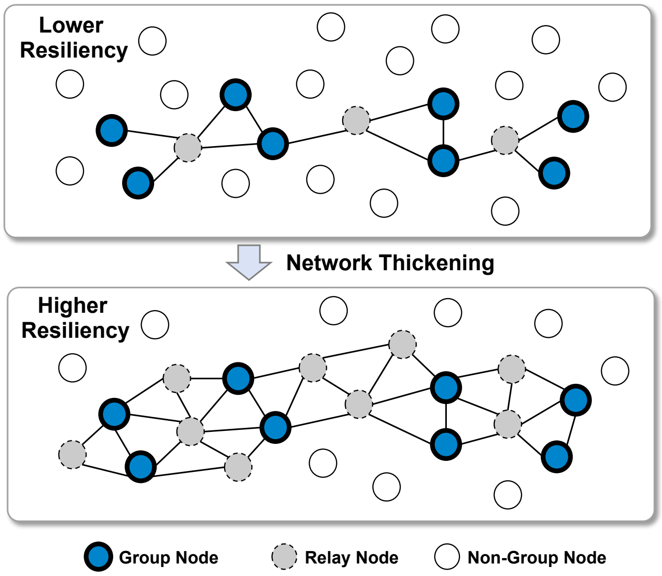


Fig. 4: Network thickening can be achieved through GCN tunable resiliency mechanism

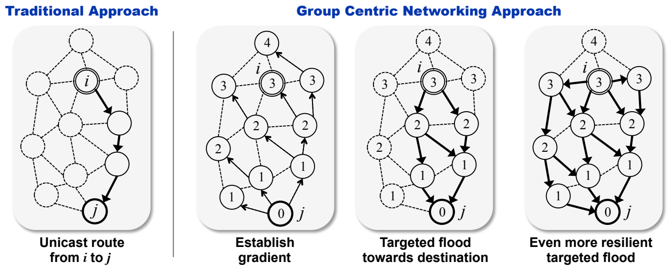

Traditional Approach
Group Centric Networking Approach
i
j
Unicast route from i to j
Establish gradient
Targeted flood towards destination
Even more resilient targeted flood

Fig. 5: GCN targeted flooding approach leverages gradients to build a corridor to direct flooded packets toward destination

group against packet loss and mobility. The effect of tunable resiliency on GCN was evaluated by examining the (1) connectivity of the group when users are mobile, and (2) how reliably and efficiently messages can be delivered in the presence of packet loss and mobility. The results in [5] demonstrates that by sending out group discovery messages only once every 100 seconds, 99% of group nodes are reachable despite mobility.

C. Targeted Flooding

The group discovery and tunable resiliency GCN mechanisms discovers group members and forms a resilient one-to-all communication pattern between all of them. Sending all messages to the entire group, however, is not always efficient. For example, a group of special operations forces may want to exfiltrate data to a single data collector via a many-to-one traffic pattern. Alternatively, some group member may want to query a subset of users, or have one-to-one communication with one other user. The *targeted flooding* mechanism enables these additional traffic patterns in a resilient manner without requiring additional control data.

In GCN, each transmitted packet (data or control) is tagged with the originating node's ID and a hop count from the source. This hop count is incremented for each retransmission and each node that overhears a new message stores and updates the local distance information (i.e. hop count) to each source. Each overheard message, therefore, provides a constant refresh of distance information without the need for dedicated control messages.

GCN's targeted flooding mechanism uses the distance information gathered from overhead packets to create a distributed gradient field towards each of the group members. To do this, the source specifies and includes in the header, a maximum retransmit distance (MRD) value. When a relay node hears a packet with a particular destination, it looks at the packet's MRD value, and if that value is greater than or equal to its own distance from the destination, it will rebroadcast the packet with the MRD field decremented by one. Adjusting the MRD value increases or decreases the resiliency. The result is that packets are flooded through a narrow corridor toward some particular destination. More details can be found in [5].

III. Performance Evaluation

To evaluate the feasibility of GCN on real-world systems, we implemented GCN as an Android process and deployed the technology on 90 mobile phones scattered throughout 2 floors of our facility. Figure 6 shows the distribution of group nodes nodes, which are randomly distributed, on 1 floor as well as an example test. In this test, 23 group nodes participated in the network and one packet per second was sent from all group nodes to all group nodes for 5 minutes. We compared packet delivery success rate and bytes transmitted over-the-air with GCN, Simplified Multicast Forwarding (SMF) [6], Optimized Link State Routing (OLSR) [7], and the Babel routing protocol [8].

As can be seen from Figure 6, GCN delivered the most packets successfully (close to 75%) and significantly more than OLSR and Babel. The maximum delivery success in this test was capacity limited. SMF floods the entire network with data resulting in higher delivery success than OLSR and Babel if available capacity is available, but still lower than GCN. In comparing overall bytes transmitted over-the-air, GCN is much more efficient, using only 10% of the amount of bandwidth required compared to SMF and over half the amount compared to OLSR and Babel. While this particular use case shows gains with GCN over traditional IP MANET-based approaches on real-world systems, it does not exploit GCN-specific capabilities such as localizing traffic to geographic regions and interest groups as well as support for other traffic patterns (many-to-one and many-to-many). Additional testing is currently being conducted on the mobile phone network and detailed simulation results can be found in [5].

IV. Discussion

GCN was designed to provide resilient, bandwidth efficient communication to users participating in interest groups. There are numerous applications to military tactical edge networks as well as limitations. Military tactical edge networks are mobile and must operate without infrastructure and in disruption,

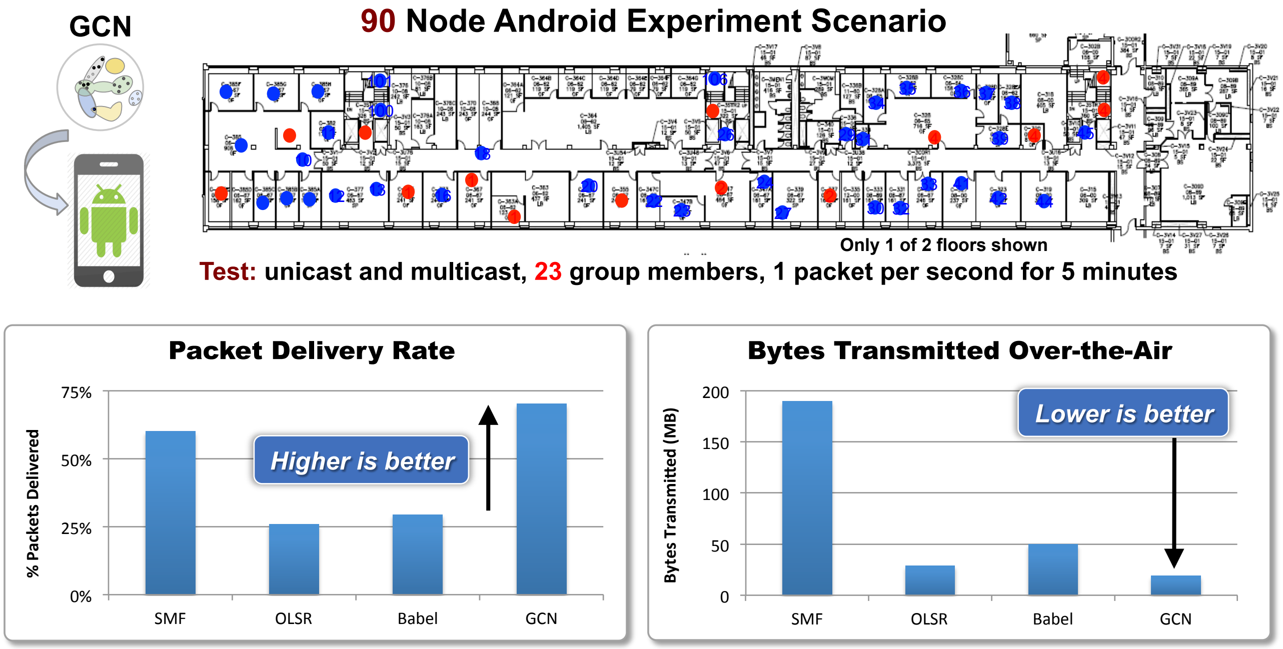


Fig. 6: GCN delivers more successful packets with lower network load than traditional IP approaches in 90 node android network

interference, and lossy environments. Additionally, much of the collaboration between users is within groups limited by geographic location. Because of potential for adversary attack and disruption, there are several unique and varying requirements based on the mission and platform. In this section, we discuss some applications and limitations of GCN on tactical edge networks.

A. Geographically Localized Communications

GCN communications are localized to the area around interest groups. The group discovery mechanism ensures that data is only sent to those interested in the information (vs. blindly broadcasted) and because military networks are geographically localized and collaborate in force structure, GCN data dissemination is inherently geographically localized. Additionally, collaboration can span multiple groups. For instance, a 4-ship may be sharing sensor data collaboratively while one of the 4-ships may be collaborating with a command and control (C2) aircraft. Each node can potentially be part of dozens of groups with different collaborators. Each of the groups can have different network resiliency requirements and information sharing requirements. GCN flexibility to dynamically join and leave groups enables flexible communications in tactical edge networks.

B. Efficient and Resilient Communications

Military tactical edge networks are typically bandwidth limited and lossy. In such environments, redundancy ensures resiliency. Protocols like SMF which flood the network are very resilient toward mobility and link loss, but suffer from high network load. GCN attempts to mitigate this by 1) only transmitting data to those interested in the data, 2) localizing transmissions, 3) building corridors of flooding, and 4) activating additional relays as needed. Because the level of resiliency varies per application, each collaborative group can tune the network for its tolerances.

C. Dynamic Network Adaptation

In traditional IP networks, routing parameters such as protocol *hello intervals*, *link state advertisement intervals*, etc. are set prior to the mission and fixed throughout the deployment. Even when no application is running or when nodes require operation in radio-silence mode, these messages are sent from the network layer. In GCN, applications set parameters that determine the amount of group discovery reach, the network resiliency, and the thickness of targeted flooding schemes on a *per-group* basis. This paradigm enables some applications that require less resiliency to activate fewer relays and those that require more resiliency to thicken the network. Additionally, different phases of the mission may require different network effects. For instance, when stealth fighters are operating outside of the threat area, they may desire to exchange messages liberally. When they enter the threat area, they may choose to stop all messages. GCN enables dynamic network adaptation on a *per-group* basis, giving greater fidelity in tactical mission planning.

D. Group ID Mapping

In GCN, interest groups are identified by a group ID. While GCN provides efficient group discovery and resilient information dissemination between groups, it does not specify how groups are formed or how group IDs are mapped. GCN expects another mechanism to give context and meaning to groups. For instance, in Link 16, statically defined network participation groups (NPGs) are used to identify types of traffic. Group IDs could potentially be formed around named data objects [9], traditional IP multicast group mappings, Link 16 NPGs, or other approaches. GCN's flexibility enables broad applicability to current and future tactical use cases.

E. Legacy Interoperability

Legacy military networks are fairly stove-pipped in nature and vertically integrated [2]. Furthermore, military networks often take decades to evolve due to long platform integration times. GCN interoperability with legacy networks may require a dual-stack approach where translators at various layers of the "stack" move data from GCN-enabled networks to legacy networks. Additionally, message gateways are typically used to translate information from one network to another. The challenge with gateways is to understand what information should be relayed from one network to another (with different message formats and technologies) and what platform should perform the gateway function such that the network is not overwhelmed with redundant data. This is done today with a lot of pre-planning. GCN can potentially alleviate these issues by mapping messages and application data to group IDs and leveraging the GCN group discovery mechanism to dynamically discover who is interested in the data.

F. Information/Content Centric Networks

In recent years, there's been a large push to move forward information-centric networks [9], [10]. In information centric networks, the network acts like a database where users query for a set of data and the network returns the content. The user does not care where the content comes from and could have been cached on a local node so long as the content arrives. GCN naturally lends itself to the information centric paradigm in that GCN does not specify what constitutes a group ID. Group IDs can be mapped to named data objects, content identifiers, or any type of identifier. GCN merely provides an efficient and resilient dissemination mechanism.

G. Directional and Heterogeneous Networks

To achieve resilience, GCN leverages the broadcast nature of transmissions to overhear and relay. While many tactical systems, particularly ground systems like soldier radio waveform (SRW) [11] and legacy airborne tactical systems like Link 16 are omni-directional systems, there has been a large push in recent years to move toward directional systems for increased capacity and lower probability of detection. To support these systems, GCN requires minimal extensions in its tunable resiliency mechanism. Specifically, GCN overhears messages and dynamically determines whether to relay the message or not based on a tunable resiliency parameter. The determination to relay is performed on the receiver. In directional systems, however, explicit transmissions need to be made to each neighbor and typically only one node overhears a message. The result is that the tunable resiliency determination of relay must occur at the sender. In other words, the sender chooses how many neighbors to relay the message to based on the level of resilience required.

Another consideration is that many tactical systems are moving towards leveraging heterogeneous radio systems [12] to provide additional links and paths through the system. In such cases, GCN would need to be extended to understand link characteristics of each system and dynamically adjust resilience based on heterogeneous links.

H. Security Architecture

Typical tactical communications systems have a plaintext (i.e. red) side and a cipher text (i.e. black) side separated by a COMSEC device. The COMSEC device encrypts all data going from red to black. In past systems, there is often a routing protocol running on the black side which efficiently converges on routes, and another protocol running on the red side which doubles the overhead. Care is taken to reduce the overhead and so often times, black routing information is passed to the red side to minimize discovery. GCN simplifies this problem significantly because the only identifier passed between red and black is the group ID. Algorithms can also be applied to the group ID such that the mapping from red to black changes over time, enabling additional security.

I. Traffic Prioritization

GCN currently does not have mechanisms to prioritize certain traffic over others in the event the medium is saturated. Additional work is needed to extend GCN to support traffic and/or content prioritization.

V. Conclusions

In this paper, we consider a new class of networking approaches called group-centric networks and its potential to address the needs of military tactical edge information sharing. Group-centric networks are characterized by a set of users or devices that are grouped by an inherent set of "interests" that are dependent on the tasks they are performing. Additionally, the majority of message exchanges between users are within some local area and long-distance traffic is only a small faction of the overall communications. Group-centric networks enable different traffic patterns between users such as one-to-one (traditional unicast), one-to-many (traditional multicast), many-to-one (exfiltration approaches), and many-to-many (data fusion).

Additionally, we examine a group-centric network protocol called Group Centric Networking (GCN) to realize the concept and demonstrate potential gains against current IP MANET approaches. GCN leverages three mechanisms (group discovery, tunable resiliency, and targeted flood) that enable potentially enables resilient and scalable multi-hop wireless communications for military tactical edge networks that collaborate as a group in local regions. We also present an instantiation of GCN on a 90 node android network and compare the performance results to SMF, OLSR, and Babel. The results show that GCN achieves near-capacity delivery success with 10-50% the network load. Furthermore, GCN can be extended to support information network concepts and is compatible with traditional tactical network security architectures.

Finally, we discuss implications of GCN as it applies to tactical edge networks by first examining the benefits and synergies with current use cases, followed by potential limitations. GCN enables tactical edge users to dynamically evolve the network depending on the phase of the mission or application-level requirements. It also provides easy extension to information-centric network paradigms and as a straightforward path into current security architectures. Although GCN has several benefits and is the first realization of group-centric networks, there are several areas of potential extension. These areas include: using GCN in a multi-channel, heterogeneous radio system, using GCN with systems of directional smart-antennas, and extensions to support additional resiliency at higher layers of the stack. Additional work is needed to address these limitations.

References

[1] B.-N. Cheng, J. Wheeler, and B. Hung, "Internet Protocol Header Compression (IPHC) Technology and Its Applicability on the Tactical Edge," *IEEE Communications Magazine*, October 2013.

[2] B.-N. Cheng, F. J. Block, B. R. Hamilton, D. Ripplinger, C. Timmerman, L. Veytser, and A. Narula-Tam, "Design Considerations for Next-Generation Airborne Tactical Networks," *IEEE Communications Magazine*, May 2014.

[3] DoD MIDS Program Office, "System Specification (SS) for Link 16 Waveform for the Multifunctional Information Distribution System Joint Tactical RAdio System (MIDS JTRS)," DoD MIDS International Program Office, Tech. Rep. SS-J-10002 Rev B, April 2007.

[4] R. Ramanathan, R. allan, P. Basu, J. Feinberg, G. Jakllari, V. Kawadia, S. Loos, J. Redi, C. Santivanez, and J. Freebersyser, "Scalability of mobile ad hoc networks: Theory vs practice," in *IEEE Military Communications Conference, MILCOM*, 2010.

[5] G. Kuperman, J. Sun, B.-N. Cheng, P. Deutsch, and A. Narula-Tam, "Group Centric Networking: A New Approach for Wireless Multi-Hop Networking to Enable the Internet of Things," in *arXiv*, 2015.

[6] J. Macker *et al.*, "Simplified multicast forwarding," Internet Engineering Task Force, RFC 6621, 2012. [Online]. Available: http://tools.ietf.org/html/rfc6621

[7] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," Internet Engineering Task Force, RFC 3626, 2007. [Online]. Available: http://www.ietf.org/rfc/rfc3626.txt

[8] J. Chroboczek, "The Babel Routing Protocol," Internet Engineering Task Force, RFC 6126, April 2011. [Online]. Available: http://www.ietf.org/rfc/rfc6126.txt

[9] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A Survey of Information-Centric Networking," in *IEEE Communications Magazine*, 2012.

[10] Z. Cao, M. French, R. Krishnan, J. Ng, D. Talmage, and Q. Zhang, "Content-Oriented Mobile Edge Technology: System Integration Framework and Field Evaluation," in *IEEE Military Communications Conference, MILCOM*, 2014.

[11] *Soldier-Level Integrated Communications Environment (SLICE) Soldier Radio Waveform (SRW) Functional Description Document (FDD) Version 1.4*, U.S Army CERDEC, January 2004.

[12] B.-N. Cheng, R. Charland, P. Christensen, L. Veytser, and J. Wheeler, "Evaluation of a Multi-hop Airborne IP Backbone with Heterogeneous Radio Technologies," *IEEE Transactions on Mobile Computing*, vol. 13, no. 2, pp. 299–310, Feb. 2014.